

UNCLASSIFIED

STATEMENT FOR THE RECORD

**BY
MR. JOHN A. RUSSACK**

**PROGRAM MANAGER
INFORMATION SHARING ENVIRONMENT
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

**BEFORE THE
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT
COMMITTEE ON HOMELAND SECURITY**

HEARING TITLED

"FEDERAL INITIATIVES FOR HOMELAND SECURITY INFORMATION SHARING"

NOVEMBER 8, 2005

UNCLASSIFIED

INTRODUCTION

Chairman Simmons, Ranking Member Lofgren, and distinguished members of the subcommittee, I consider it an honor to be here today to update you on my efforts to implement the recommendations that Congress prescribed in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. We need not look far to the tragic events of September 11, 2001, to understand that we have significant work remaining to fully implement an information-sharing environment that more effectively supports our national counterterrorism mission. I believe there is not an issue more seminal to the security of our nation than information sharing. I accepted this responsibility because I am committed to doing something about it. This task is too large and much too important for me to do it alone, which is why Congress must remain fully engaged in this effort and provide its leadership, support, and necessary guidance to transform our current capabilities into a better, more effective Information Sharing Environment (ISE).

In August of 2004, the President issued Executive Order 13356 to ensure that terrorism information is shared broadly among federal agencies; state, local, and tribal governments; and the private sector. Then in response to the IRTPA, on April 15, 2005, the President designated me as the Program Manager (PM) for the Information Sharing Environment, and on June 2nd, the President directed that the PM be part of the Office of the Director of National Intelligence (ODNI).

On June 15th, I submitted a preliminary report to the President and Congress—the first deliverable mandated by IRTPA. This report identified five broad issues affecting information sharing that will largely define the agenda for my office over the next two years. On October 25th, the President issued EO 13388 establishing the Information Sharing Council (ISC), and I now have an approved charter authorizing the ISC to assist and advise the President and myself in carrying out our duties as described in section 1016 of IRTPA. On October 27th, Ambassador Negroponte sent a letter to Department Secretaries and Agency Directors requesting representatives to the ISC. While the institutional foundations are in place to allow us to make significant progress in the way we share terrorism information, a number of hurdles that exist that will require hard work and leadership to surmount. We are committed to identifying and removing all impediments that prevent us from providing the best possible information to decision makers, at whatever level.

In fact, significant efforts have been made to meet Congress' intent in making information sharing a priority. In consultation with the ISC, and state, local, and private sector representatives, I will formulate policies and guidelines to enable broader sharing of terrorist information, develop an ISE concept of operations and architecture, and prepare for the President an implementation plan for the Information Sharing Environment. Once the plan is adopted, my office will manage, support, monitor, and assess ISE implementation by Federal departments and agencies, and regularly report my findings to Congress.

I have organized my office around three major priorities: policy, technology, and business process, and I have recruited and staffed senior positions for each of these key areas. My office is currently staffed with 11 Federal employees, with eight more in the hiring process;

UNCLASSIFIED

we are further augmented with six on site contractors. The quality of personnel now onboard is outstanding, and is representative of all of the agencies and departments of the Federal government--not just the Intelligence Community (IC). I am on track to obtain additional Federal Government employees and achieve our established personnel goal of twenty-five.

The following are representative accomplishments associated with the stand-up of my office:

- I distributed a Request For Information (RFI) to industry on August 18, 2005, to develop an Electronic Directory Service (EDS) or the functional equivalent required by section 1016(b) of the IRTPA. Forty-eight responses were received from potential developers, and are now being analyzed. These inputs may provide the basis for a Request for Proposal (RFP).
- The Institute for Defense Analyses (IDA) has been under contract to my office since July 2005 to perform a comprehensive review of the existing ISE. The resulting December 2005 report will serve as a key point of departure for implementing the ISE.
- In October, I established three ISE steering groups: (1) Information Access, Search, and Exploitation; (2) ISE Governance and Collaboration; and (3) Security and Privacy. The ISC and I will look to these groups to be the primary focal points for integrating all work in their respective issue areas. The steering groups will leverage and track ongoing work to avoid duplication, integrate results, and report progress to myself and the ISC. In addition, they will identify any issues not being addressed, assign priorities, and propose options for resolving them.
- My office is engaged in identifying a number of promising information sharing technology pilot programs, including two particularly promising projects – one with the New York Federal Bureau of Investigation (FBI) Field Office on a Sensitive But Unclassified (SBU) technology demonstration; the other a project with our Department of Energy (DOE) national laboratories, to leverage both analytic and technical expertise to counter the potential for nuclear terrorism.

ROLE OF THE PROGRAM MANAGER

The ISE will be a national information-sharing environment enabling frictionless terrorism information access. It is a combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, state, local, and tribal entities and the private sector to facilitate information sharing, access, and collaboration among users to combat terrorism more effectively.

The IRTPA required the President to designate a program manager (PM) “responsible for information sharing across the Federal Government,” with government-wide authority. Section 1016(f) outlines the duties and responsibilities that were assigned to me as the Program Manager:

UNCLASSIFIED

- Plan for and oversee the implementation of, and manage, the Information Sharing Environment;
- Assist in the development of policies, procedures, guidelines, rules and standards as appropriate to foster the development and proper operation of the Information Sharing Environment; and
- Assist, monitor, and assess the implementation of the Information Sharing Environment by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

Since September 11, 2001, significant progress has been made to improve the Nation's ability to access, integrate, and share terrorism-related information. Legislative changes and executive orders have reduced some of the barriers to sharing. New organizations such as the National Counterterrorism Center (NCTC), the Department of Homeland Security (DHS), the Terrorist Screening Center (TSC), and state and local intelligence fusion centers have bolstered our national effort to collect, analyze, and disseminate information. My office will build on these collective capabilities. The ISE that exists today must be more robust and interconnected to ensure our national security. Policies, rules, architectures and systems, which support specific individual missions, must be adjusted to enhance frictionless, rapid information access. One of the functions of my office will be to coordinate these individual efforts so that they are uniformly directed towards a single collective effort to share information throughout the mission space.

The ISE of the future must transform, integrate and connect existing elements into a cohesive framework by providing common policies, guidelines, systems, and architecture. Leveraging existing initiatives will be critical to getting this task done in an expedited manner. The challenge herein is that terrorism information is not limited to intelligence. The counterterrorism mission will require the integration of information from homeland security, private sector, law enforcement, financial, and bio-surveillance, to name a few. Each of these classes of information possesses its own unique legal requirements, business rules, technical architectures, standards, and capabilities. Therefore, coordinating this effort will be a critical function of my office.

Creating an ISE that effectively facilitates the flow of information across agency, jurisdictional, and domain boundaries must be enabled by technology. It is key to note that technology is not the solution but an enabler, and technologies currently exist to meet this challenge. Rewriting the business rules for this new ISE will require that we address all the impediments to sharing – policy, culture, and roles, missions and responsibilities. Critical to this effort is leadership. One of my roles is that of a catalyst in implementing the ISE, creating the conditions necessary to optimize information sharing. Ultimately Federal agencies and all of our non-federal partners will each have to share the responsibility and provide the necessary leadership to make the ISE we need. The success of this effort will be directly related to the commitment that each agency makes to change its culture from the need-to-protect to the need-to-share.

STATE, LOCAL, TRIBAL GOVERNMENT AND THE PRIVATE SECTOR

We must better support the key new partners in our counterterrorism efforts: the state, local, and tribal governments, and private sector. I intend to fully support the efforts currently underway at the Department of Homeland Security, the Department of Justice (DOJ), and the Department of Defense (DOD) to provide actionable information to their customers.

The current federal system (processes, protocols and technology capabilities) that supports the sharing of terrorism-related information and intelligence between Federal, state, local, and tribal governments, and the private sector is not cohesive and has led to the development of an ad-hoc patchwork of informal and formal networks to facilitate the sharing of information among local partners. These “networks” include a variety of organizational structures and processes for gathering, analyzing, and sharing terrorism-related information and intelligence. Most states have begun to establish statewide intelligence fusion centers to serve as central hubs to facilitate statewide efforts to gather and analyze terrorism-related information, blend it together, and then produce and disseminate intelligence products used to support homeland security related prevention, response and recovery activities (operational and planning).

I recognize that statewide and major urban area information fusion centers have the potential to be a critical part of the ISE. Thirty states have information “fusion” centers and 11 more are being developed. Identifying best practices with regard to establishing a fusion capacity within the state and local information-sharing environment will significantly contribute to the ISE implementation. I further support the efforts by the DHS, DOJ, and other relevant Federal entities to coordinate their domestic information and intelligence efforts with these fusion centers.

Effectively engaging state, local, tribal, and private sector authorities in the ISE development process will require overcoming significant frustration by local entities over the perceived “lack of progress” in establishing a national terrorism information sharing system. I know that Members regularly hear from their local law enforcement entities, first responder groups, and the private sector on the continuing lack of coordination among federal entities. We must work together more seamlessly at the Federal level in order to better leverage the capabilities that the state, local, and tribal entities bring to the counterterrorism effort.

Our ISE planning efforts will take into account that:

- Counterterrorism-related prevention, response and recovery efforts carried out at the state, local, and tribal levels must be integrated into their “all-crimes, all-hazards” approach to homeland security;

UNCLASSIFIED

- In addition to supporting investigations, terrorism-related intelligence is used at the state, local, and tribal levels to support a broad array of activities, including: completion of jurisdictional risk assessments; allocation of fiscal resources; response and recovery planning efforts; and critical infrastructure protection; and
- State, local, tribal, and private sector authorities need more unclassified information and intelligence, and the traditional Federal emphasis on producing and disseminating classified information impedes the effective use of that information to support multi-disciplinary prevention, response, and recovery efforts.

Another important initiative that I will continue to expand is the use of information access pilot programs at the state and local levels. We currently have two pilot programs that involve the FBI and DOE. The FBI New York Office's Special Operations Division currently utilizes handheld wireless devices for field operations. In addition to emails and alerts, the devices can be used to access various databases. The objective of the FBI pilot project is to facilitate enhanced communications among counterterrorism personnel and provide rapid wireless access to SBU data sources. The DOE is sponsoring a pilot project that will apply technical analytic expertise to intelligence pertaining to nuclear terrorism. The project has established a core group of nuclear expert analysts across five DOE national laboratories, focused on providing both long-term, strategic analysis of the supply-side of nuclear terrorism and better short-term tactical intelligence, with an additional objective of improving potential collection opportunities. Central to the success of this effort is the sharing of all relevant sensitive reporting with these national laboratories. Pilot programs provide valuable end-user input to the technical development of the ISE, and significant buy-in that will be crucial for cultural change in the information-sharing environment.

ELECTRONIC DIRECTORY SERVICES

I am required to provide an electronic directory service (EDS) or a functional equivalent that meets the requirements and objectives of the IRTPA, based on a community-wide, enterprise architecture, to focus on a broad range of threats. The EDS must accommodate increasing numbers of sources, and be implemented utilizing existing technologies and ongoing EDS and collaboration efforts. The EDS will provide a set of capabilities to inform ISE users of the resources available for collaboration, including professionals from across the IC, Federal, state and local governments, as well as private industry, academia and allied countries. Capabilities, such as people and organizational information, will be made available on a real-time basis to all ISE users, employing traditional search and drill-down functionality.

The EDS implementation will be achieved through a three-phased approach. The first phase will start small by leveraging existing IC counterterrorism directory services such as Intelligence Community Full Service Directory (IC FSD) and the National Counterterrorism Center Online (NOL) directory.

The second phase will include people/organization listings from Federal organizations such as use of capabilities of the Department of Justice - Global Justice Information Sharing Initiative, Regional Data Exchange (R-DEx), Law Enforcement Online (LEO), the Regional

UNCLASSIFIED

Information Sharing System (RISS) and the Department of Homeland Security – Transportation Security Administration Operating Platform.

The third phase will include state/local governments, private sector, academia and Allied countries. The use of capabilities such as the Department of Homeland Security Regional Information Exchange System (HSIN), state fusion centers and New York State Directory Service (NYSDS) would provide immediate initial capability.

SUMMARY

I believe there is no higher priority for our national security than the issue of information sharing. Congress has provided us the mandate through legislation; the President has provided us the leadership and further guidelines; now we must finalize the work of transforming our information-sharing environment into one that works more effectively for all. Thousands of men and women work tirelessly to protect this nation from terrorist threats. It is important for us to provide them and other decision makers with the best possible information to do their job to protect the people and interests of the United States against another terrorist attack.

It is important to emphasize that my function in all of this is to serve as an *enabler* for better access and collaboration. Each department and agency with a counterterrorism mission will retain their current roles. Our collective task is to lead the effort to better clarify these roles, missions, and responsibilities, and implement an ISE that better supports their efforts.

In closing, I would like to leave you with some key priorities in establishing the Information Sharing Environment:

- It is absolutely essential that information flow in two directions. The "*environment*" we create needs to provide better access to Federal terrorism information at the state and local levels—however, and of equal importance, it must also provide mechanisms to allow valuable information gathered by state and local officials to be used by Federal agencies.
- The Intelligence Community no longer serves as the single source for information, particularly where terrorism information is involved. Customers can and do get their information elsewhere. Consumers of terrorism information demand expertise; are substance oriented; and require each of us engaged in countering terrorism to operate in a "fast forward, value added mode."
- While it's true that some in the Intelligence Community have historically regarded protection of intelligence sources and methods as more important than sharing the information, it's an impediment that must be overcome. Protection and sharing of information are not mutually exclusive. We can and will share the information we collect and analyze, while protecting our most sensitive sources and methods.
- I recognize that there are potentially serious issues affecting privacy, civil liberties and the equities of state and local governments that will need to be addressed before we achieve the two-way flow of information. Close collaboration between officials at all levels will be

UNCLASSIFIED

essential to develop the policies and processes we need. Although some terrorism information must always be classified, our goal has to be that we provide as much as possible at the unclassified level.

- One of my responsibilities is to identify any impediments to effective information sharing and to remove them. Consumers of terrorism information must receive all the information they need from us, quickly and free of unnecessary restrictions.

My office, under the leadership of the DNI, is committed to creating an effective ISE that extends beyond the Intelligence Community. This task will include the development of nationwide policies that will enable individual Federal agencies and key partners to begin to adopt practices that reflect effective information sharing capabilities and procedures. Our state, local, and tribal governments and private sector entities must be full partners in this effort

Mr. Chairman, I appreciate the opportunity to provide this subcommittee an update on the activities of the Program Manager's Office and look forward to your questions. Thank you.